

NMCI Security – protection at highest level available

CHIEF WARRANT OFFICER 2 THOMAS W. ROGOWSKY
DIRECTOR OF CSSF

This is the third installment of a four-part series of articles designed to inform individuals of the upcoming transition to the Navy Marine Corps Intranet environment.

For as long as there have been computers there have been hackers. In the infancy of the computer generation, hackers were generally seen as thrill-seeking Robin Hoods who were more apt to be mischievous than malevolent. But those innocent times are gone.

Today’s hackers are more insidious and the damages they inflict are far more costly. In 1999, the Explorer virus caused damages worldwide in excess of \$1.02 billion and the Melissa virus carried a price tag of \$1.1 billion.

In 2000, the Love Bug resulted in more than \$8.75 billion in damages and in 2001 NIMDA, Code Red, and Sir Cam and other viruses/worms had a net cost of over \$12.9 billion. Virus attacks have become a near constant threat,

with each new attack being more sophisticated and complex than the one before.

A primary benefit of the Department of the Navy transition to the Navy Marine Corps Intranet will be the ability to implement an enterprise approach to Information Assurance, incorporating the most modern detection measures available to prevent viruses from infiltrating data files, applications, e-mail, and the network as a whole.

To do this, the EDS/NMCI team has developed a multi-layered defense that includes built-in protections, email protections, and application and Internet security.

Built-In Protections
Our current defensive Information Assurance posture protects the Depot’s network against malicious codes, spam e-mails, and active attacks.

NMCI will implement similar tactics and strategies to continue this stewardship of high network availability while actively minimizing the Depot’s vulnerability from internal and external threats.

Each time you log onto the NMCI network, the system will automatically launch Norton AntiVirus protection programs to scan all media and checks for viruses. The application is continuously monitored and updated to ensure that if a virus is discovered, it will be prevented from spreading within the NMCI network.

The application is also designed to apply corrective measures to remove the virus from your workstation.

Virus protection upgrades within NMCI are downloaded to your workstation automatically while you are logged on the network.

Anti-virus software is loaded at the server level so that all data transmitted within NMCI, and data received externally, is intensely scrutinized to protect the network and individual workstations.

Defending Against E-Mail Assaults

Most viruses attack and compromise computer networks through an e-mail assault.

Since most e-mail viruses

are contained in attachments, the NMCI restricts some file extensions from being sent through the NMCI. The system also includes filters for spam e-mail to prevent spam from being automatically sent to distribution lists groups on the network.

If a virus penetrates an e-mail account, the system will quarantine the infected message, run the appropriate virus software and eradicate the contaminated message to keep it from circulating in the NMCI environment.

Enhanced Internet and Application Security

NMCI security enhancements also include protection from virus assaults launched through the Internet.

When visiting Web sites external to NMCI, continual virus scanning occurs at the Web server level, using firewalls to filter data and allowing only NMCI traffic to access system resources.

The standardization of NMCI applications adds the security or knowing the software was received from a trusted source. Downloading

software or data from a non-NMCI machine brings the added risk of infecting the workstation or network.

As an added measure of protection, Application Security for NMCI workstations begins when the workstation is first loaded with the standard package of application software, known as the “Gold Disk.”

Attempting to install non-standard applications will trigger an alert to the system administrator that a workstation is being compromised. The workstation will be placed in quarantine and an EDS NMCI team technician will be mobilized to determine the cause and extent of the problem.

Through its multi-layered IA approach, NMCI will provide better security and protection for all NMCI workstations.

The NMCI security provides:

- Detection**
 - 24x7 surveillance against unauthorized intrusions
 - Defends bases or sites against internal as well as external threats
 - Inoculates systems with

state-of-the-art, anti-virus detection tools

- Inspection**
 - Continually monitors the network, assessing potential threats to the environment
 - Offers new tools and activities to inspect and protect the system

- Protection**
 - State-of-the-art firewall protection
 - Protection is standard across the NMCI enterprise
 - Provides comprehensive password procedures to safeguard information
 - Assures information is safe — even when using government-approved applications located outside NMCI

- Reaction**
 - Alerts security personnel of virus contamination in the environment 24x7
 - Quarantines contaminated files, greatly limiting potential damage to work
 - Reports unauthorized intrusions to Navy and Marine Corps security team
- The final installment of this series, NMCI Hardware and Software, will be appearing next week.*

SEMPER FIT, Continued from Page 1

educated on the statistics and risk factors, and that they follow up on their physician’s recommendations. With as much media attention that breast health has received in the past few years, you would think that everyone would be taking it seriously. Unfortunately, there are some who do not.”

Even though early detection is the best defense against breast cancer, some things such as regular exercise, maintaining a healthy weight and limiting alcohol intake can help lower the risks, according to Dilliard.

Americans can wear pink ribbons on their lapels to help support the fight against breast cancer and the search for its cure throughout the month of October. The ribbon has become a symbol for the cause and also a way of honoring survivors and those lost to the disease. To find out more about breast cancer, log onto the American Cancer Society Web site at www.cancer.org. To find out more about National Breast Cancer Awareness Month, log onto www.nbcam.org.

To find out more about the Relay for Life and how you can volunteer, contact Dilliard at 228-7010.

Happy Birthday Marines!

Birthday Ball dates:

RTR Sgt. & Below	WFTBn. Sgt. & Below	H&SBn.Sgt. & Below	Depot Officer’s Ball	Depot Staff NCO Ball
Saturday, Nov. 1	Friday, Nov. 7	Friday, Nov. 14	Saturday, Nov. 8	Saturday, Nov. 15
Tickets: \$8	Tickets: \$10	Tickets: \$14	Tickets: \$30	Tickets: \$11
Cocktails: 6:30 p.m.	Cocktails: 7:30 p.m.	Cocktails: 5:00 p.m.	Cocktails: 6:30 p.m.	Cocktails:7:30 p.m.
Ceremony: 8:30 p.m.	Ceremony: 8:30 p.m.	Ceremony: 6:30 p.m.	Ceremony: 7:30 p.m.	Ceremony: 8:30 p.m.
POC: Sgt. Blutcher, 228-3154	POC: Company office	POC: Company office	POC: Company office	POC:Company office

Two photo packages will be offered:

- Package A will include: 1-8x10, 2-5x7 and 8 wallet for \$29
- Package B will include: 2-5x7 and 8 wallets for \$23